(12) PATENT
(19) AUSTRALIAN PATENT OFFICE

(11) Application No. AU 199928111 B2
(10) Patent No. 758892

(54) Title
An apparatus for conducting a secure electronic transaction

(51)[6] International Patent Classification(s)
G06F 017/60 H04L 009/32

(21) Application No: 199928111 (22) Application Date: 1999.05.12

(30) Priority Data

| (31) Number | (32) Date | (33) Country |
|---|---|---|
| 9801578 | 1998.07.02 | SG |

(43) Publication Date : 2000.01.20
(43) Publication Journal Date : 2000.01.20
(44) Accepted Journal Date : 2003.04.03

(71) Applicant(s)
Advent Television Ltd

(72) Inventor(s)
Robert Jefferies Chatfield

(74) Agent/Attorney
GRIFFITH HACK,256 Adelaide Terrace,PERTH WA 6000

(56) Related Art
EP 779587
WO 97/49055
WO 96/12242

**EDITORIAL NOTE**

**APPLICATION NUMBER - 28111/99**

**This specification does not contain an Abstract page.**

P/00/011
Regulation 3.2

AUSTRALIA

PATENTS ACT 1990

# COMPLETE SPECIFICATION FOR A

# STANDARD PATENT

Name of Applicant: ADVENT TELEVISION LTD

Address of Applicant: 510 Thomson Road #12-04
SLF Building
Singapore 298135

Actual Inventor: Robert Jefferies CHATFIELD

Address for Service: Griffith Hack, Patent and Trade Mark Attorneys, 6th Floor, 256 Adelaide Terrace, Perth, Western Australia, 6000.

Standard Complete Specification for the invention entitled:

**AN APPARATUS FOR CONDUCTING A SECURE ELECTRONIC TRANSACTION**

Details of Parent Application for Divisional Applications:

Singapore Patent Application No. 9801578-7 dated 2 July 1998

The following is a full description of this invention, including the best method of performing it known to me:-

## TITLE

An Apparatus For Conducting A Secure Electronic Transaction.

## FIELD OF THE INVENTION

This invention relates to an apparatus for conducting a secure electronic transaction, and to a method of performing an electronic transaction.

## BACKGROUND ART

The increasing popularity of the Internet has seen the emergence of electronic commerce. The rate of acceptance of electronic commerce has been much slower than the growth rate of the Internet itself, primarily because of consumer concerns regarding security and a lack of awareness of where products may be purchased.

## SUMMARY OF THE INVENTION

In accordance with a first aspect of this invention, there is provided an apparatus for conducting a secure electronic transaction, comprising:

a server including a secure data area in which data regarding vendible products and services are stored, said server being connectable to a broadcast network and being arranged to broadcast information regarding said vendible products and services during use, said information including at least some of said data, and a unique identifier for each vendible product and service; and

at least one client arranged to receive said information via the broadcast network during use, each client including means for establishing, and temporarily securing, a return communications link with the server so as to facilitate communication of financial information regarding a transaction between the client and the server;

whereby communication between each client and the server uses the broadcast network for communications from the server to the client and the return communications link for communications from the client to the server, the information including the unique identifier being received by the server from the client when the return communications link is established, and wherein the means for temporarily securing the communications link with the server is arranged to exchange public encryption keys between the client and the server, and the server is arranged to forward said financial information to a financial institution by a further secure communications link whereupon

said financial institution conducts the financial transaction.

In one arrangement, the server is arranged to broadcast a first public encryption key with the information regarding each product and service, the client is arranged to encrypt a second encryption key using the first encryption key and communicate said encrypted second encryption key to the server and the server is arranged to decrypt and recover said second encryption key for use in communicating with the client.

In an alternative arrangement, the server receives a first public encryption key from the client and the server is arranged to broadcast a second encryption key to the client using the broadcast network.

In this alternative arrangement, it is preferred that the server is arranged to encrypt the second encryption key using the first encryption key, and the client is arranged to decrypt and recover said second encryption key for use in communicating with the server.

Preferably, said broadcast network is wireless.

Preferably, the broadcast network forms part of a digital television broadcast network.

Preferably, said unique identifier is generated from a pseudo-random sequence.

Preferably, a seed for the pseudo-random sequence is provided by said financial institution.

Preferably, said return communications link is a telephone line.

Preferably, said data regarding vendible products and services includes data regarding the vendor of said products and services, said server being arranged to communicate information regarding said vendor to said financial institution.

Preferably, said server is arranged to continuously broadcast information regarding said vendible products and services.

Preferably, said client comprises a portable or mobile computer.

Preferably, said computer includes a digital television receiver.

Preferably, said computer includes a card reader arranged to read a public encryption key from a card disposed in use in said card reader.

Preferably, the server is arranged to create a receipt and an audit trail using the information received from the client and data stored in the secure data area regarding the vendor and the product or service, and the unique identifier associated with the transaction.

In accordance with a second aspect of this invention, there is provided a method for conducting a secure electronic transaction, comprising the steps of:

using a broadcast network to broadcast information regarding vendible products and services, said information including for each vendible product and service a unique identifier;

establishing a return communications link between a client and a server, whereby communication between the client and the server uses the broadcast network for communications from the server to the client and the return communications link for communications from the client to the server;

temporarily securing the return communications link by exchanging public encryption keys between the client and the server;

using said temporarily secured communications link to communicate financial information regarding the transaction; and

forwarding said financial information to a financial institution via a further secure communications link.

Preferably, the step of establishing a temporarily secure communications link comprises the step of exchanging public encryption keys.

## DETAILED DESCRIPTION OF THE EMBODIMENT

The embodiment is directed towards an apparatus for conducting a secure electronic transaction. The apparatus includes a server having a secure data area. In the secure data area, data structures referred to as "proposers" of transactions are stored. Each proposer data structure includes the following data: description of the product or service, pricing data, availability and delivery data, and financial data on the vendor, such as details of the bank account to deposit funds from transactions. Each proposer may also include multimedia data containing advertising information, such as images, sounds and the like. A proposer data structure exists for each product or service.

The server is connected to a digital television broadcast network and is arranged to continuously broadcast descriptive information on the products and services contained in the proposer data structures. The information broadcast by the server regarding each product or service includes the description of the product or service, pricing data, availability and delivery data, and multimedia data (if any) from the proposer data structure, and a unique identification code generated from a pseudo-random sequence.

The broadcast information can be received anywhere within the broadcast area, thereby avoiding the need to forward information on each product and service to each client separately.

Within the broadcast area, a client receives the information regarding the proposers by the broadcast information. The client includes a processing means in the form of a computer having a digital television receiving card provided therein. The computer receives the broadcast information and displays the same to a user. Thus, the user can view the products and services at his or her leisure.

When the user wishes to conduct a transaction in relation to one or more products or services, the computer establishes a return communications link with the server. In this regard, since the broadcast network is a transmit only system, a return communications link is required for communications from the client to the server. In the embodiment, the return communications link takes the form of

a telephone line. The computer establishes a communications link with the server via the telephone line and transmits the unique identification code of each good or service in which the user is interested. The computer also transmits the client's public encryption key for the purposes of establishing a secure communications link. The server receives the information via the return communications link. The server then communicates the server's public encryption key to the client via the broadcast network.

Information regarding the transaction is then exchanged between the client and the server using the broadcast network as the forward communications link between the server and the client and the telephone line as the return communications link between the client and the server. The public encryption keys which have been exchanged by the client and server are used for the purposes of establishing a temporarily secure connection. Information exchanged includes the quantity of each product and service desired to be purchased by the user and the user's financial information, such as credit card details and so forth.

Upon receipt of the information from the client, the server forwards financial information regarding the transactions to a financial institution via a secure communications link. In this regard, the financial information includes the user's financial information such as the credit card details, and also includes the vendors financial information obtained from the corresponding proposer data structure. The financial transfer is effected by the financial institution.

Once confirmation has been received from the financial institution that the transaction has been successfully completed, a receipt is generated and forwarded to the user via the broadcast network using the encryption key.

The server further creates an audit trail using the financial information received from the user, the financial information stored in each proposer the subject of the transaction and the unique identification associated with each product and service. The audit trial is stored within the secure data area.

For the purposes of this specification it will be clearly understood that the word "comprising" means "including but not limited to", and that the word "comprises" has a corresponding meaning.

It should be appreciated that this invention is not limited to the particular embodiment described above.

## CLAIMS

1. An apparatus for conducting a secure electronic transaction, comprising:

a server including a secure data area in which data regarding vendible products and services are stored, said server being connectable to a broadcast network and being arranged to broadcast information regarding said vendible products and services during use, said information including at least some of said data, and a unique identifier for each vendible product and service; and

at least one client arranged to receive said information via the broadcast network during use, each client including means for establishing, and temporarily securing, a return communications link with the server so as to facilitate communication of financial information regarding a transaction between the client and the server;

whereby communication between each client and the server uses the broadcast network for communications from the server to the client and the return communications link for communications from the client to the server, the information including the unique identifier being received by the server from the client when the return communications link is established, and wherein the means for temporarily securing the communications link with the server is arranged to exchange public encryption keys between the client and the server, and the server is arranged to forward said financial information to a financial institution by a further secure communications link whereupon said financial institution conducts the financial transaction.

2. An apparatus as claimed in claim 1, wherein the server is arranged to broadcast a first public encryption key with the information regarding each product and service, the client is arranged to encrypt a second encryption key using the first encryption key and communicate said encrypted second encryption key to the server, and the server is arranged to decrypt and recover said second encryption key for use in communicating with the client.

3. An apparatus as claimed in claim 1, wherein the server receives a first public encryption key from the client and the server is arranged to broadcast a second

encryption key to the client using the broadcast network.

4. An apparatus as claimed in claim 3, wherein the server is arranged to encrypt the second encryption key using the first encryption key, and the client is arranged to decrypt and recover said second encryption key for use in communicating with the server.

5. An apparatus as claimed in any one of the preceding claims, wherein said broadcast network is wireless.

6. An apparatus as claimed in any one of the preceding claims, wherein the broadcast network forms part of a digital television broadcast network.

7. An apparatus as claimed in any one of the preceding claims, wherein said unique identifier is generated from a pseudo-random sequence.

8. An apparatus as claimed in claim 7, wherein a seed for the pseudo-random sequence is provided by said financial institution.

9. An apparatus as claimed in any one of the preceding claims, wherein said return communications link is a telephone line.

10. An apparatus as claimed in any one of the preceding claims, wherein said data regarding vendible products and services includes data regarding the vendor of said products and services, said server being arranged to communicate information regarding said vendor to said financial institution.

11. An apparatus as claimed in any one of the preceding claims, wherein said server is arranged to continuously broadcast information regarding said vendible products and services.

12. An apparatus as claimed in any one of the preceding claims, wherein said client comprises a computer.

13. An apparatus as claimed in claim 12, wherein said computer includes a digital television receiver.

14. An apparatus as claimed in claim 12 or 13, wherein said computer includes a card reader arranged to read a public encryption key from a card disposed in use in said card reader.

15. An apparatus as claimed in any one of the preceding claims, wherein the server is arranged to create a receipt and an audit trail using the information received from the client and data stored in the secure data area regarding the vendor and the product or service, and the unique identifier associated with the transaction.

16. A method for conducting a secure electronic transaction, comprising the steps of:

using a broadcast network to broadcast information regarding vendible products and services, said information including for each vendible product and service a unique identifier;

establishing a return communications link between a client and a server, whereby communication between the client and the server uses the broadcast network for communications from the server to the client and the return communications link for communications from the client to the server;

temporarily securing the return communications link by exchanging public encryption keys between the client and the server;

using said temporarily secured communications link to communicate financial information regarding the transaction; and

forwarding said financial information to a financial institution via a further secure communications link.

17. An apparatus for conducting a secure electronic transaction substantially as hereinbefore described.

18. A method for conducting a secure electronic transaction substantially as hereinbefore described.

Dated this 2nd day of January 2003

ADVENT TELEVISION LTD

By Its Patent Attorneys
GRIFFITH HACK

Fellows Institute of Patent and Trade Mark Attorneys of Australia.